Attachment H - System Technical Requirements & Specifications

Anticipated System Use and Deployment

System Usage Profile/System Performance

The responsiveness of the system is of great importance. The system will be house data from multiple agencies and will be accessed via various data portals to be defined in later phases. The record sets are vast and the solution must be able to accommodate multifaceted data calls without a drop in performance. The warehouse and subsequent structures should optimize data access.

Hardware and Hosting

The current expectation is to provide the hosting of the system through the IOT data center. Bidders should make recommendations regarding hardware array and software configuration for the solution they propose including consideration for load balancing, redundancy, failover, and backup and recovery.

User Roles

The INK system should include various levels of data access with the ability to create new roles based on business needs. Example role levels are listed below:

- Record level access to de-identified data
- De-identified record level access at home agency; aggregate level access for other data
- Aggregate level access
- Record level access at home agency including identifiable information
- Record level access to cross agency identifiers

Priority Key

Each requirement has a priority for development. All items listed are required. By prioritizing requirements, it is recognized that not all features have an equal effect on the success or utility of the Teaching and Learning Portal. The priority levels are defined below:

1. **Vital—**the system will not function acceptably without this function.

2. **Important—**lack of this function will have a major effect on the performance or functionality of the system.

3. **Useful—**the function would frequently assist the user in performing his or her activities. Other means could be used, but at the expense of time or money.

A list of the requirements for respondents' reference is also presented in the technical proposal, **Attachment F**.

Technical Requirements

All work done under the resulting contract will meet all technical, security, accessibility, and privacy standards in effect with the Indiana agencies at the time of implementation including but not limited to those outlined below. Expectations regarding identity management, security, and data confidentiality are addressed below:

- **Identity Management** — identity Management Solution should be part of the bidder response to ensure the appropriate level of security to the data that will be available in INK.

- **Security** — the successful vendor will develop a solution in accordance with established security and privacy policies of the State of Indiana agencies. Attention to security of user accounts and account information should include the considerations outlined in the requirements section below.

- **Confidentiality** — the confidentiality of data is of utmost concern for the State of Indiana. Security standards must be in place and student data confidentiality must be followed. The guidelines for data use and access as outlined in the Family Education Rights and Privacy Act (FERPA) must be followed along with applicable portions of Article 7, Rule 38, Indiana's Special Education rules, other applicable Indiana statutes (e.g. those applying to workforce data, etc.), and any other statute, rule or policy pertaining to data security.

CODE	COMPONENT	COMPONENT ACTION	PRIORITY
TR.1	***Technical Requirements***	**Provide** multidimensional datasets to be utilized in online analytical processing using industry standard	1
TR.2	***Technical Requirements***	Role-based access to system functionalities and data	1
TR.3	***Technical Requirement***	**Provide** data diagrams with mapped data dependencies	
TR.4	***Technical Requirements***	**Develop** data schemas with consideration for national standards (e.g., CEDS) and with regard to the agencies' data dictionary	1
TR.5	***Technical Requirements***	**Develop** system for data cleanup processes	1

CODE	COMPONENT	COMPONENT ACTION	PRIORITY
TR.6	***Technical Requirements***	**Provides** functionality at various levels (e.g. state, county, school district, school/institution and economic growth region levels)	1
TR.7	***Technical Requirements***	**Provides** built in data dictionary functionality.	1
TR.8	***Technical Requirements***	**Industry Best Practices:** Configured for easy updates and preservation	1
TR.9	***Technical Requirements***	**Industry Best Practices:** Employs production quality publication and system monitors methods (e.g. Extract, Translate and Load packages; Redgate deploy)	1
TR.10	***Technical Requirements***	**Industry Best Practices:** Enhances data quality by applying necessary constraints	1
TR.11	***Technical Requirements***	**Industry Best Practices:** Utilizes industry standards for data security and will maintain confidential data in an appropriate manner to ensure compliance with all applicable state and federal laws	1
TR.12	***Technical Requirements***	**Industry Best Practices:** Utilizes industry standards for user group management (e.g. LDAP)	1
TR.13	***Technical Requirements***	**Industry Best Practices:** Provides for backup and recovery consistent IOT architecture and policy requirements	1
TR.15	***Technical Requirements***	All work done under the resulting contract will meet all technical, security, accessibility, and privacy standards in effect for all partnering agencies at the time of implementation, including but not limited to: Section 508, FERPA, and other federal and state laws.	1
TR.16	***Technical Requirements***	**Provide** for reasonable exceptions to system rules such as: a) Individuals with varying access levels depending on data source and b) ad hoc data requests	1
TR.17	***Technical Requirements***	**Utilize** best practices for non-identifiable record identification	1

CODE	COMPONENT	COMPONENT ACTION	PRIORITY
TR.18	***Technical Requirements***	**Provide** security functions to limit access to authorized users.	1
TR.19	***Technical Requirements***	**Provide** computerized audit trail of all users who have accessed or updated a record, including date / time stamps and IP address.	1
TR.20	***Technical Requirements***	**Support** a secure user authentication process based on industry best practice for the data being accessed that complies with IOT architecture and system requirements (potentially include integration with existing network credentials).	1
TR.21	***Technical Requirements***	**Provide** transactional and final data tables to allow for the load, approval, and publication of data	1
TR.22	***Technical Requirements***	**Provide** mechanism to allow for specific spans of data release for public consumption (e.g. 5 years of data available)	1
TR.23	***Technical Requirements***	**Industry Best Practice:** Utilize industry standards to support data analytics and reporting	1
TR.24	***Technical Requirements***	**Provide** system that is scalable to include additional state agencies	1
TR.25	***Technical Requirements***	**Provide** a robust matching algorithm that is portable and expandable to encompass current partner agencies as well as potential additional state agencies	1